Available online at https://www.ijasrd.org/

International Journal of Advanced Scientific Research & Development

Vol. 06, Iss. 03, Ver. I, Mar' 2019, pp. 34 – 38

e-ISSN: 2395-6089
p-ISSN: 2394-8906

SECURE MEDICAL DATA COMPUTATION USING VIRTUAL_ID AUTHENTICATION AND FILE SWAPPING

K. Satheesh Kumar[1*], N. Anusiya[2], P. Mahalakshmi[2], and **P. Manimegalai[2]**

[1] Asst. Prof., Department of Computer Science and Engineering, University College of Engineering, Thirukkuvalai, Nagapattinam, India.

[2] Student, Department of Computer Science and Engineering, University College of Engineering, Thirukkuvalai, Nagapattinam, India.

ARTICLE INFO

Article History:

Received: 19 Mar 2019;
Received in revised form:
30 Mar 2019;
Accepted: 30 Mar 2019;
Published online: 10 Apr 2019.

Key words:

Hashing,
Homomorphic Encryption,
NTRU,
Medical Application,
File Swapping,
IDS.

ABSTRACT

PHR provides users with a great deal in leakage of sensitive information. However, securing the sensitive medical data also brings very serious security problems, especially for the data security which is stored in the medical cloud data. Once the data is leaked to a third party, then the data privacy has become a major problem, mainly such as authentication, availability of data, confidentiality etc., and which is to be taken into consideration very effectively. An authentication scheme based on virtual smartcard using hashing function for medical data is proposed to solve the problem of in which the illegal users access the resources of servers. Here, we also maintain PHR sensitive data in the cloud by using file swapping concept. Once the user access the data. The user data will be swapped into different places by file swapping concept, so the file will be more secured and no one can hack or theft our data.

INTRODUCTION

Healthcare data security is very much essential in the Health Insurance and Accountability Act Rules. The HIPAA belongs to Security Rule that requires fully covered entities to assess data security manage by conducting a risk assessment, and implement a risk management program to address any vulnerabilities that are identified. In 2015 there were 750 breaches found and the 193 million personal records opened to make fraud. In June 2016 alone, more than 11 million health care records were exposed because of cyber-attacks and over millions of data where hacked in 2018. Looking at these numbers, it is obvious that cyber and data security is a major concern to health care.

Cite this article as: Kumar, S. K., Anusiya, N., Mahalakshmi, P., & Manimegalai, P., "Secure Medical Data Computation using Virtual_ID Authentication and File Swapping". *International Journal of Advanced Scientific Research & Development (IJASRD), 06* (03/I), 2019, pp. 34 – 38. https://doi.org/10.26836/ijasrd/2019/v6/i3/60305.

*** Corresponding Author:** K. Satheesh Kumar, satheesh@aucetk.edu.in

In the existing system the medical data in cloud is secured by using GPU_Accelerated homomorphic encryption scheme which is used for securing only the medical Cloud data, the major problem is Authentication(in every aspects such as big data, cloud computing, and etc.),and identification of file location after decryption may allow hacker to access data .

In this paper we proposed an idea in order to avoid such problem we have used using hashing technique[1] with SHA-2 for authentication and file swapping[2] for changing the location of the decrypted file. We have used IDS[3] for monitoring unauthorized access and NTRU[4] based homomorphic encryption[5] for cloud data.

HASHING TECHNIQUE

A hash value is unique which helps to identify secret information. The hash function is the collision-resistant is needed to find data which will generate the same hash value. There are two types of functions in hashing which are listed as follows

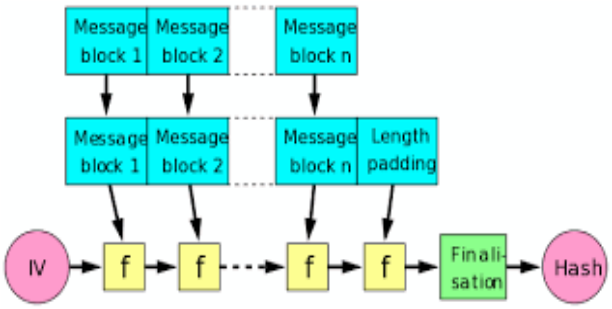
1) Cryptographic hash function
2) Provably secure hash function

The provably secure hash function is very slow but it is very secured. For generating the very large hash value the collision resistance is accomplished. But cryptographic is too fast as well as secure, hence we have used it for our implementation.

Example: SHA-2 is most popular cryptographic function which is designed by National Security Agency (NSA). It contain six different types of hashing algorithm, they are

- SHA-256
- SHA-512
- SHA-224
- SHA-384
- SHA-512/224
- SHA-512/256

It has undergone 64-rounds of hashing and also it calculate hash code (i.e.,) 64-digit hexadecimal number.



2.1 Input Format

A single alphanumeric string is denoted by s.

2.2 Constraints

$6 \leq |s| \geq 20$ and String s consists of alphabetic letters (i.e., [a-z A-Z]), and decimal digits (i.e., 0 through 9) only.

2.3 Output Format

Print the SHA-256 encryption value of s on a new line.

NTRU SCHEME

The NTRU operation will increases quadratically and it is a open source public key cryptosystem which uses lattice based cryptography for encryption and decryption of data, whereas RSA operation increases as cubically, hence NTRU is chosen which consist of two algorithm

1) NTRUEncrypt
2) NTRUSign

NTRUEncrypt, which is used for encryption, and NTRUSign, which is used for digital signatures and the attacks are resisted by using Shor's algorithm and its performance is much better than others. It was placed in public domain in 2017 and it can be used by software under the GPL[6][7]. Here the NTRUEncrypt is preferred to make safe of cloud storage data in an Encrypted form.

NTRU BASED HOMOMORPHIC EVOLUTION

In this section, we describe our implementation in detail. We know that prince cipher is most relevant for Homomorphic evolution. Then later we implemented the shallow circuit and for implementation we need to select the optimal parameter based on DHS FHE scheme

While permitting a shallow circuit implementation picking up a lightweight block cipher will provide the efficient encryption which means the level of multiplication should be minimized. Therefore we turn around ourself to use the lightweight block ciphers[8]. There are two linear factors which increase the number of multiplication is: size and the complexity of s-boxes and if higher linearity occur then it results in higher degree terms. PRESENT[9] it has simple s-boxes for individual s-box resulting in shallow circuit. Where PRESENT is less optimal because of higher rounds. Prince is a recent model of block cipher[10] which has same complexity for s-boxes but it has 12 round for the efficient process, the more complex layer does not make a problem because it does not introduce any new binary multiplication.

The complexity of different lightweight cipher can be overviewed and note that the cipher depth is determined by consecutive levels of binary AND-statement. There are two types of software-oriented ciphers they are, SEA and HEIGHT. Feistel-structure and high number of rounds results in high depth circuit which make bad choice. The addition of mod 2 n gives significant output due to high nonlinearity. In FHE supports for evaluating integer operation and not to the mixed integer hence bit-oriented operation is required by

most block cipher. Hence, the hardware oriented cipher such as Present and Prince is mostly preferred. Example, the evolution of few rounds in parallel, since the bits are processed in consecutive rounds. AES offers a low depth due to the low number of rounds. In resent 30 implementation of AES gives rise to several multiplications, instead depth 40 implementation is used in current practice. The ANF (Algebraic Normal Form) is used to represent the optimal representation of the S-boxes in the form of XOR or AND statements.

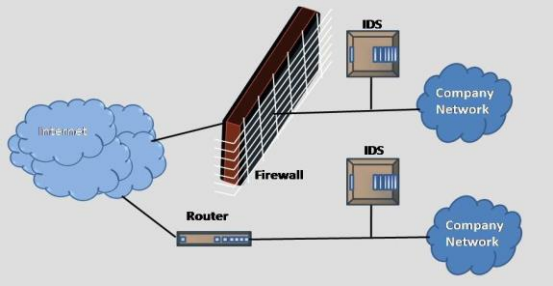
FILE SWAPPING

The file swapping for exchanging access database in single IP is as same as the swapping of two numbers concept.

We all know that our data is hacked by the unauthorized user if they find the location of our file, where it is found in a user's single IP and hence in order to avoid this hacking we introduced the concept called FILE SWAPPING[11].

Here the file swapping concept implements after a decryption of a file, when the file is accessed by user it is swapped into other place within singleIP and make secure arrangements.

INTRUSION DETECTION SYSTEM (IDS)



An Intrusion Detection System (IDS) is a device or software application which is used for monitoring a network of a systems or for malicious activity. It sends the activity of unauthorized user information to an administrator or otherwise it collects centrally using security information. Any malicious activity or violation is typically reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system is used to combines outputs from multiple sources, and the alarm filtering techniques is used to distinguish malicious activity from false alarms.

Intrusion Prevention Systems (IPS), also known as intrusion detection and prevention systems (IDPS) are network security appliances which is used for monitoring the network activities are network security appliances that monitor network or system activities for malicious activity.

The IPS is classified into 4 different types which are listed as follows

1) Network-based intrusion prevention system (NIPS)
2) Wireless intrusion prevention system (WIPS)
3) Network behavior analysis (NBA)
4) Host-based intrusion prevention system (HIPS)

It uses three different types of detection methods in Intrution Prevention System namely, Signature-based detection, Statistical anomaly-based detection, Stateful protocol analysis detection.

The main functions of intrusion prevention systems are to identify malicious activity, log information about the intrusion detection system.

CONCLUSION

We formulated, optimized, and implemented an NTRU-based variant of the HE scheme of which achieves much slower growth of noise, and thus much better parameters than previous HE schemes. Compared to the work in, our GPU Implementation (GM204 Maxwell Architecture) achieves a speedup of 6085xin Ctxt multiplication, which represents the bottleneck for most HE schemes. Representative medical applications, namely Pearson Goodness-of-fit test, Cochran-Armitage Test for Trend (CATT), predictive analysis, and relational operations were implemented and scored speedups of 160.9x, 162.9x, 80000x, and 12.2x, respectively.

REFERENCES

[1] Konheim, A., (2010). "7. Hashing for Storage: Data Management". Hashing in Computer Science: Fifty Years of Slicing and Dicing. Wile Interscience. ISBN 9780470344736

[2] Turcan, E., (2002), "Peer-to-Peer: The Third Generation Internet". Retreived from http://csdl.computer.org/comp/proceedings/p2p/2001/1503/00/15030095.pdf

[3] Vilela, Douglas W. F. L.; Lotufo, Anna Diva P.; Santos, Carlos R. (2018). Fuzzy ARTMAP Neural Network IDS Evaluation applied for real IEEE 802.11w data base. 2018 International Joint Conference on Neural Networks (IJCNN). IEEE. doi:10.1109/ijcnn.2018.8489217. ISBN 9781509060146.

[4] Robertson, Elizabeth D. (August 1, 2002). "RE: NTRU Public Key Algorithms IP Assurance Statement for 802.15.3" (PDF). IEEE. Retrieved February 4, 2013.

[5] S. Carpov, R. Sirdey, "Another compression method for homomorphicciphertexts", Proceedings of the 4th InternationalWorkshop on Security in Cloud Computing, 2016.

[6] https://www.securityinnovation.com/company/news-and-events/press-releases/security-innovation-makes-ntruencrypt-patent-free

[7] https://github.com/NTRUOpenSourceProject/ntru-crypto#is-ntru-patented

[8] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, and L. Uhsadel. A survey oflightweight-cryptography implementations. IEEE Design Test of Computers, 24(6):522{533, Nov 2007.

[9] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B.Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An Ultra-Lightweight BlockCipher, pages 450{466. Springer Berlin Heidelberg, Berlin, Heidelberg, 2007.

[10] Julia Borgho, Anne Canteaut, Tim G□uneysu, Elif Bilge Kavun, MiroslavKnezevic, Lars R. Knudsen, Gregor Leander, VentzislavNikov, ChristofPaar, Christian Rechberger, Peter Rombouts, S_ren S. Thomsen, and Tolga Yal_c_n.PRINCE{ A Low-Latency Block Cipher for Pervasive Computing Applications,pages 208{225. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[11] "Copyright and Peer-To-Peer Music File Sharing: The Napster Case and the Argument Against Legislative Reform". murdoch.edu.au. March 2004.]

[12] Jump up to:a b Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF). Computer Security Resource Center (800–94). Retrieved 1 January 2010.